(TS//SI//REL) Peeling Back the Layers of TOR with

EGOTISTICALGIRAFFE

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371101

Overall Classification

This briefing is classified

TOP SECRET//COMINT//REL USA, FVEY

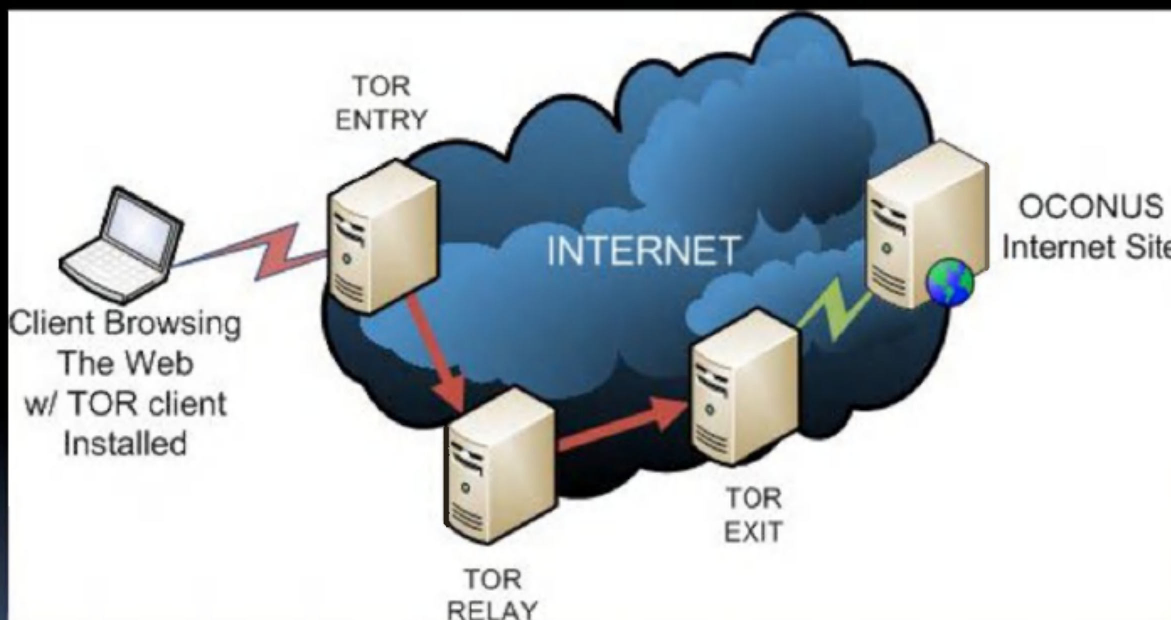
(U) Overview

- (U) What is TOR?
- (S//SI//REL) The TOR Problem
- (TS//SI//REL) EGOTISTICALGOAT
- (TS//SI//REL) EGOTISTICALGIRAFFE
- (U) Future Development

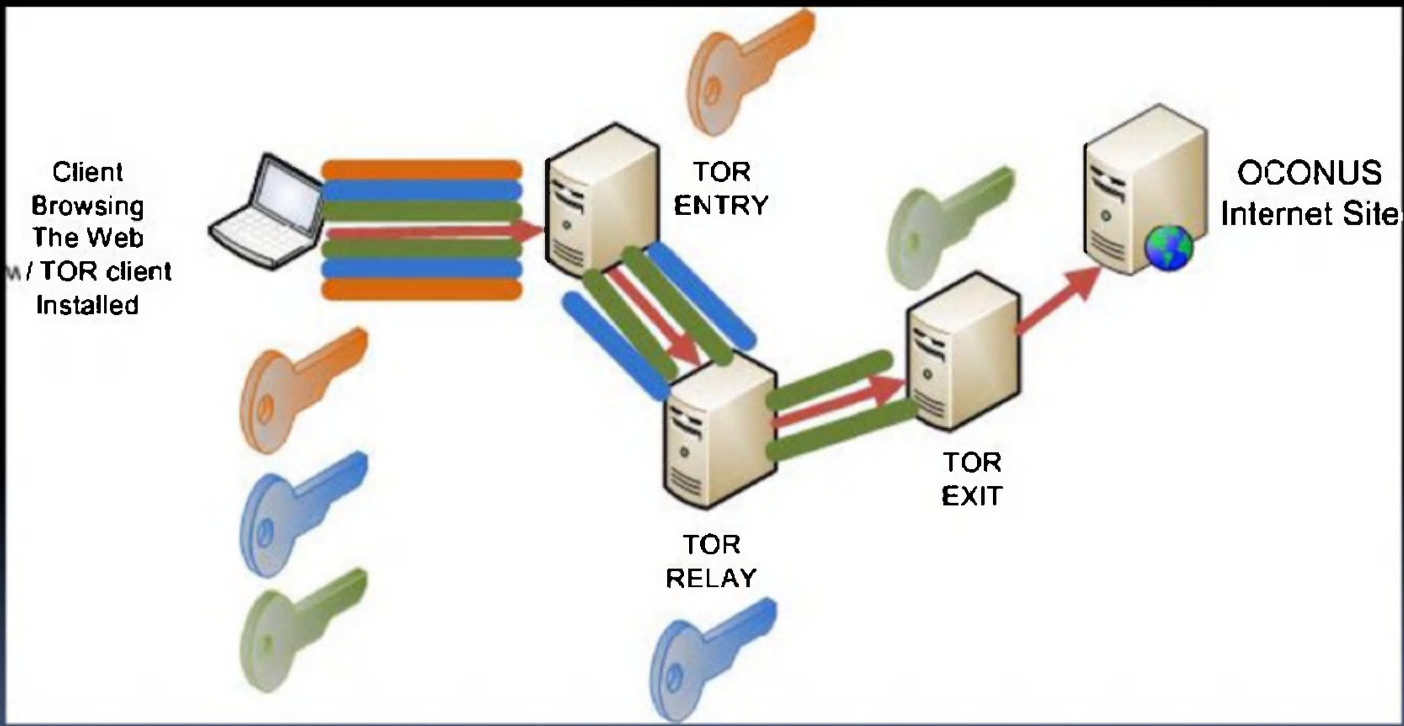
(U) What is TOR?

- (U) "The Onion Router"
- (U) Enables anonymous internet activity
  - General privacy
  - Non-attribution
  - Circumvention of nation state internet policies
- (U) Hundreds of thousands of users
  - Dissidents (Iran, China, etc)
  - (S//SI//REL) Terrorists!
  - (S//SI//REL) Other targets too!

(U) What is TOR?


TOR
ENTRY
INTERNET
OCONUS
Internet Site
Client Browsing
The Web
w/ TOR client
Installed
TOR
EXIT
TOR
RELAY

(U) What is TOR?


Client
Browsing
The Web
w/ TOR client
Installed
TOR
ENTRY
OCONUS
Internet Site
TOR
EXIT
TOR
RELAY

(U) What is TOR?

- (U) TOR Browser Bundle
  - Portable Firefox 10 ESR (tbb-firefox.exe)
  - Vidalia
  - Polipo
  - TorButton
  - TOR
  - "Idiot-proof"

(S//SI//REL) The TOR Problem

- (TS//SI//REL) Fingerprinting TOR
- (TS//SI//REL) Exploiting TOR
- (TS//SI//REL) Callbacks from TOR

(TS//SI//REL) Fingerprinting TOR

Windows XP
Firefox 10.0.5 ESR?

- 32-bit Windows 7
- Firefox/10.0

64-bit Mac OS X
Firefox 10.0.4 ESR?

- 32-bit Windows 7
- Firefox/10.0

Ubuntu 11.10
Firefox 10.0.7 ESR?

- 32-bit Windows 7
- Firefox/10.0

64-bit Windows 7
Firefox 10.0.10 ESR?

- 32-bit Windows 7
- Firefox/10.0

Windows 7
Firefox 10.0, not running TOR?

- 32-bit Windows 7
- Firefox/10.0

(TS//SI//REL) Fingerprinting TOR

(TS//SI//REL) BuildID gives a timestamp for when the Firefox release was built

20121024073032

Year	Month	Day	Hour	Min	Sec
2012	10	24	07	30	32

(TS//SI//REL) tbb-firefox's BuildID:

0

(TS//SI//REL) Fingerprinting TOR

- (TS//SI//REL) TorButton cares about TOR users being indistinguishable from TOR users
- (TS//SI//REL) We only care about TOR users versus non-TOR users
- (TS//SI//REL) Thanks to TorButton, it's easy!

(S//SI//REL) The TOR Problem

- ~~(TS//SI//REL) Fingerprinting TOR~~
- (TS//SI//REL) Exploiting TOR
- (TS//SI//REL) Callbacks from TOR

(TS//SI//REL) Exploiting TOR

- (TS//SI//REL) tbb-firefox is barebones
  - Flash is a no-no
  - NoScript addon pre-installed…

    …but not enabled by default!
  - TOR explicitly advises against using any addons or extensions other than TorButton and NoScript
- (TS//SI//REL) Need a native Firefox exploit

(TS//SI//REL) Exploiting TOR

- (TS//SI//REL) ERRONEOUSINGENUITY
  - Commonly known as ERIN
  - First native Firefox exploit in a long time
  - Only works against 13.0-16.0.2
- (TS//SI//REL) EGOTISTICALGOAT
  - Commonly known as EGGO
  - Configured for 11.0-16.0.2...

    ...but the vulnerability also exists in 10.0!

(U) EGOTISTICALGOAT

- (TS//SI//REL) Type confusion vulnerability in E4X
- (TS//SI//REL) Enables arbitrary read/write access to the process memory
- (TS//SI//REL) Remote code execution via the CTypes module

(TS//SI//REL) Exploiting TOR

- (TS//SI//REL) Can't distinguish OS until on box
  - That's okay
- (TS//SI//REL) Can't distinguish Firefox version until on box
  - That's also okay
- (TS//SI//REL) Can't distinguish 64-bit from 32-bit until on box
  - I think you see where this is going

(S//SI//REL) The TOR Problem

- ~~(TS//SI//REL) Fingerprinting TOR~~
- ~~(TS//SI//REL) Exploiting TOR~~
- (TS//SI//REL) Callbacks from TOR

(TS//SI//REL) Callbacks from TOR

- (TS//SI//REL) Tests on Firefox 10 ESR worked
- (TS//SI//REL) Tests on tbb-firefox did not
  - Gained execution
  - Didn't receive FINKDIFFERENT
- (TS//SI//REL) Defeated by Prefilter Hash!
  - Requests EGGI: Hash(tor_exit_ip || session_id)
  - Requests FIDI: Hash(target_ip || session_id)

(TS//SI//REL) Callbacks from TOR

- (TS//SI//REL) Easy fix
  - Turn off prefilter hashing
  - FUNNELOUT
- (TS//SI//REL) OPSEC Concerns
  - Pre-play attacks
    - PSPs
    - Adversarial Actors
  - Targets worth it?

(S//SI//REL) The TOR Problem

- ~~(TS//SI//REL) Fingerprinting TOR~~
- ~~(TS//SI//REL) Exploiting TOR~~
- ~~(TS//SI//REL) Callbacks from TOR~~